

UNITED STATES DEPARTMENT OF AGRICULTURE

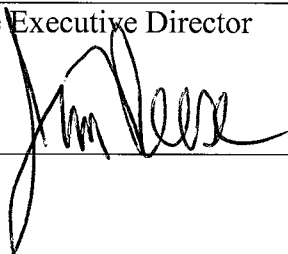
Farm Service Agency
100 USDA Suite 102
Stillwater, Oklahoma 74074-2653

OK Notice PM-1406

For: State Office and County Offices

Computer Security Rules of Behavior

Approved by: State Executive Director



1 Overview

A Background

Farm Service Agency has developed Computer Security Rules of Behavior in conjunction with OCIO-ITS. NIST and OMB A-130 require that agencies develop and distribute the Rules to all users

B Purpose

The purpose of this notice is to issue a copy of the OCIO-ITS Computer Security Rules (Exhibit 1).

2 Action

A State and County Offices

A copy of this notice and exhibit shall be provided to every FSA employee for review.

Disposal Date: January 1, 2006

Distribution: State and County Offices



United States
Department of
Agriculture

Office of the Chief
Information Officer

Service Center
Technology
Modernization
Project
Program
Management Office

1400 Independence
Ave, SW
Stop 7605
Washington, DC
20250-7605

November 22, 2004

TO: Service Center Agency Employees, Contractors, and Partners

FROM: Richard K. Roberts
Executive Project Manager
Service Center Technology Modernization Project

Frank Shehan
Chief Information Officer
Farm Service Agency (FSA)

Mary Thomas
Chief Information Officer
Natural Resources Conservation Service (NRCS)

Tom Hannah
Chief Information Officer
Rural Development (RD)

SUBJECT: Computer Security and Rules of Behavior

In recognition of the National Cyber Security Awareness Day, Office of Chief Information Officer, Information Technology Services (OCIO-ITS) and the Service Center Agencies (FSA, NRCS, and RD) would like to remind all users of their responsibilities to keep our networks safe and secure. The primary purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Well-chosen security rules and procedures are put in place to protect important assets and thereby support the overall mission of an agency.

It is extremely important that all users:

- Utilize effective passwords
- Analyze incoming e-mail
- Physically secure computers
- Protect the confidentiality of sensitive data
- Promote security awareness

USDA is an Equal Opportunity Employer

Computer Security and Rules of Behavior**Page 2**

As per Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources* and Cyber Security requirements, OCIO-ITS has developed the Rules of Behavior for the Service Center Agency user community. Refer to the accompanying brochure, "Security Expectations and Rules of Behavior," for fundamental rules regarding the importance of computer security and safety.

Please place the enclosed brochure near your workstation for easy reference. Periodically review the "Security Expectations and Rules of Behavior" to ensure your actions are consistent with computer security best practices.

EVERYONE IS RESPONSIBLE FOR COMPUTER SECURITY!

Please address any questions to Janell Duke, Security Policy Branch, OCIO-ITS, jsduke@kcc.usda.gov or (816) 926-1641.

Enclosure

Cc:

Greg Gage, Deputy Executive Project Manager, PMO
David Buckholtz, PMO
Anthony Capo, SCMI ISSPM
Brenda Dinges, RD ISSPM
Michael Sheaver, NRCS ISSPM
Brian Davies, FSA ISSPM
Janell Duke, SCMI Security Project Team, Security Awareness Team Leader

Office of the Chief Information Officer Information Technology Services



Security Expectations and Rules of Behavior

PASSWORDS

- Use alphanumeric passwords that are not easy to guess. Include special characters, if supported by the system, to make it as difficult as possible for your password to be guessed by someone else.
- Words contained in dictionaries, spelling lists, and other word lists should not be used as a password. Software programs allow hackers to breach easily constructed passwords, e.g., computer1.
- Do not choose a password that can be associated with you, such as your street address, license plate number, or name spelled backwards followed by a number.
- Protect your passwords from disclosure and change it often. Do not share your passwords with anyone else, including help desk personnel, security office, and your supervisor. Do not post your passwords anywhere in your work area, such as under your keyboard, on the monitor, or in a desk drawer.
- Your workstation must be protected from unauthorized access whenever you leave it. You must either log off, manually lock your workstation or invoke your password-protected screen saver, to ensure your unattended workstation is protected from unauthorized access.
- Change your password immediately and notify your supervisor and security office if you believe that your password might be known by someone else or that someone has gained unauthorized access into your system.

EMAIL

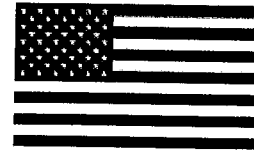
- Sending an e-mail message is like mailing a postcard – you don't know who might eventually read it, so assume everyone can.
- Address e-mail carefully. Verify you are sending the message to the correct person.
- Frequently update any e-mail distribution lists you might have created to ensure former or transferred employees are deleted from the lists.
- Verify the file name and contents of any attachment to your outgoing e-mail to ensure sensitive information is not being sent to an unauthorized individual.
- If you receive material via e-mail that is inappropriate, such as pornographic material, notify your supervisor immediately.
- To minimize the introduction of viruses, ask friends and family not to send you any e-mail messages with non-work related attachments to your government e-mail address.
- Do not open an attachment in your e-mail if you do not know the person who sent it, you were not expecting it, or if you are not familiar or comfortable with the extension for the attachment. Viruses may be embedded in the attachment, such as an attachment with the extension .exe, .pif, .com, etc. If a message you receive does not fit the normal patterns for e-mail, do not open the attachment until you verify the validity of the attachment by contacting the sender.

SENSITIVE DATA

- You are responsible for always protecting the confidentiality of sensitive data and information. Do not disclose or discuss any sensitive data or information with unauthorized individuals.
- You must refer anyone unknown to you asking questions about sensitive information to your supervisor and/or your security office.
- Access to sensitive data or information within FSA, NRCS, and RD must be kept to a "need to know" basis.
- When training, do not share any sensitive or confidential data or information with trainees that they do not need to know to perform their work responsibilities.

NOTE: "Sensitive" data includes Privacy Act information such as names, social, home addresses, etc. It also includes equipment and network configuration and IP addresses.

**Office of the Chief Information Officer
Information Technology Services**



Security Expectations and Rules of Behavior

SOFTWARE

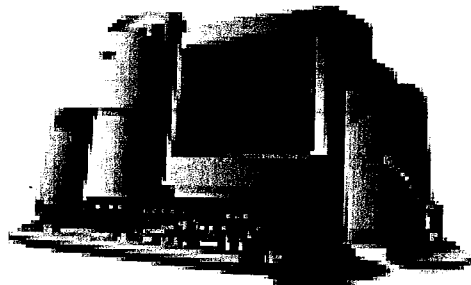
- Do not access, modify, or copy any account, file, or application that is not required to perform your official duties.
- Do not install or use unauthorized software, "peer-to-peer" software, and "file sharing" products, such as Morpheus and Kazaa, on equipment used to conduct government business.
- Do not download software from the Internet to government computers, such as freeware, shareware, or public domain software, without proper prior approval.
- Observe all software license agreements concerning issues such as distribution of software. Do not violate copyright laws. You are *personally responsible* for all costs or fines resulting from copyright infringement. This includes sharing of music and video files.

OFFICE EQUIPMENT

- Confirm the identity of anyone repairing a computer or other equipment in your area. Vendors must be escorted and monitored at all times while performing maintenance duties.
- Do not move equipment into or out of your work area or exchange computer components without required authorization.
- Double check that there is no sensitive information on your computer prior to sending it out of the office for service.
- Follow policy and take appropriate steps to thoroughly clean hard drives before equipment is reassigned, surplus, or discarded.
- Do not create any unauthorized connections to other systems or services.
- Protect computer equipment from potential hazards, such as food, drink, staples, and paper clips.
- Immediately report security incidents to your supervisor and security office, such as theft of equipment or software, or unauthorized disclosure of data or information.
- If you suspect a virus has infected your workstation, stop using it immediately, turn off its power, and immediately notify your supervisor and security office.
- Do not participate in chain letters or chat rooms, download games, files or programs, or access inappropriate or questionable Web sites.
- Scan diskettes or CDs for viruses before use.

ALTERNATE WORK SITES

- All security measures at the workplace should also be followed while working at home or a satellite work site.
- Never store sensitive information on the workstation at your alternate work site. Remember – if you use the agency access server at any time, you are using government property.
- Do not share a telephone number or remote access procedure with an unauthorized individual.



WARNING: Violation of any provision of OCIO-ITS security policies may result in disciplinary action in accordance with USDA policy and the policies of the sponsoring agency. These actions can include: access limitations, restitution for improper use, initiation of legal action, etc.